

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-069595

(43)Date of publication of application : 07.03.2003

(51)Int.Cl.

H04L 12/46

G06F 12/14

G06F 15/00

H04L 12/66

H04Q 9/00

(21)Application number : 2001-255251

(71)Applicant : SANYO ELECTRIC CO LTD

(22)Date of filing : 24.08.2001

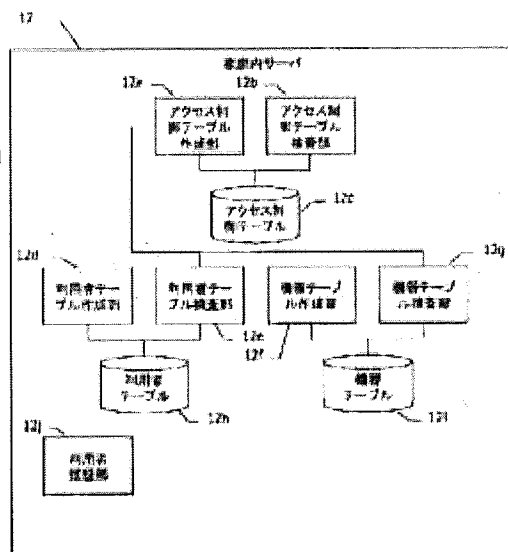
(72)Inventor : OKAMOTO MITSUNAGA
INOUE YASUAKI

(54) ACCESS CONTROL SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To perform a fine access control.

SOLUTION: A home server 12 having an access control table 12c, a user table 12h, and a device table 12i makes a decision whether or not to permit an access request after referring to contents of these tables when the access request about a customer premises equipment is received from external equipment. Especially, the approval or disapproval of the access request is predefined in detail about contents of functions of the external equipment, etc., thereby the fine access control can be done.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-69595

(P2003-69595A)

(43) 公開日 平成15年3月7日(2003.3.7)

| (51) Int.Cl. ⁷ | 識別記号 | F I | サーチコード(参考) |
|---------------------------|-------|---------------|-------------------|
| H 0 4 L 12/46 | | H 0 4 L 12/46 | M 5 B 0 1 7 |
| G 0 6 F 12/14 | 3 1 0 | G 0 6 F 12/14 | 3 1 0 K 5 B 0 8 5 |
| | 15/00 | | 3 3 0 D 5 K 0 3 0 |
| H 0 4 L 12/66 | | H 0 4 L 12/66 | B 5 K 0 3 3 |
| H 0 4 Q 9/00 | 3 0 1 | H 0 4 Q 9/00 | 3 0 1 D 5 K 0 4 8 |

審査請求 未請求 請求項の数 4 O L (全 7 頁)

(21) 出願番号 特願2001-255251(P2001-255251)

(22) 出願日 平成13年8月24日(2001.8.24)

(71) 出願人 000001889

三洋電機株式会社

大阪府守口市京阪本通2丁目5番5号

(72) 発明者 岡本 充永

大阪府守口市京阪本通2丁目5番5号 三

洋電機株式会社内

(72) 発明者 井上 泰彰

大阪府守口市京阪本通2丁目5番5号 三

洋電機株式会社内

(74) 代理人 100076258

弁理士 言田 研二 (外2名)

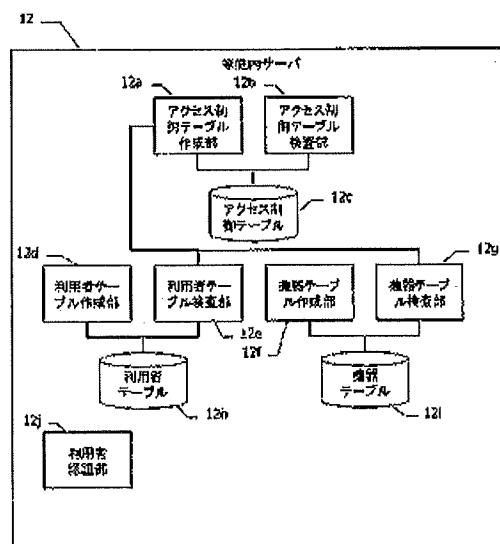
最終頁に続く

(54) 【発明の名称】 アクセス制御システム

(57) 【要約】

【課題】 きめ細かなアクセス管理を行う。

【解決手段】 家庭内サーバ12は、内部にアクセス制御テーブル12c、利用者テーブル12h、機器テーブル12iを有し、外部から宅内機器についてのアクセス要求がきたときに、これらテーブルの内容を参照してアクセス可否を判定する。特に、このアクセス可否は、機器の機能などの内容についても細かく設定されており、きめ細かい制御が行える。



(2)

特開2003-69595

1

【特許請求の範囲】

【請求項1】 内部ネットワークを介し接続された複数の機器と、

前記複数の機器のそれぞれについて、制御内容のレベルに応じアクセスの可否を決定するアクセス管理情報を記憶し、前記複数の機器に対するアクセスを管理する管理サーバと、

を含み、

前記管理サーバは、外部通信ネットワークを介し行われる、外部からの前記複数の機器へのアクセスを制御するアクセス制御システム。

【請求項2】 内部ネットワークを介し接続された複数の機器と、

前記複数の機器についてのアクセス管理情報を記憶し、前記複数の機器に対するアクセスを管理する管理サーバと、

を含み、

前記管理サーバは、外部通信ネットワークを介し接続された機器の内の1つの機器による、あるいは、前記複数の機器の内の1つの機器による、他の機器が有するオブジェクトの使用を制御するアクセス制御システム。

【請求項3】 内部ネットワークを介し接続された複数の機器と、

前記複数の機器のそれぞれについて、制御内容のレベルに応じアクセスの可否を決定するアクセス管理情報を記憶し、前記複数の機器に対するアクセスを管理する管理サーバと、

を含み、

前記管理サーバは、外部通信ネットワークを介し行われる、外部からの前記複数の機器へのアクセスを制御すると共に、外部通信ネットワークを介し接続された機器の内の1つの機器による、あるいは、前記複数の機器の内の1つの機器による、他の機器が有するオブジェクトの使用を制御するアクセス制御システム。

【請求項4】 請求項1～3に記載のシステムにおいて、

前記管理サーバは、利用者毎、または利用者のレベル毎にアクセスの可否またはオブジェクト使用の可否についてのデータを記憶しているアクセス制御システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワークに接続されている各種機器についてのアクセス制御に関する。

【0002】

【従来の技術】従来より、パソコンやネットワークサーバなどにおいては、ファイルやディレクトリに対するアクセス制御が行われている。すなわち、ファイルやディレクトリについて、自分のみの利用にしたり、無制限に

2

アクセスを許可したり、限定されたユーザについてのみアクセスを許可するというアクセス権を設定することができる。例えば、特開2001-60972号公報では、機器の機能とユーザのレベルを組み合わせたアクセス制御方式を提案している。

【0003】また、特開2001-60972においては、外部通信回線を介する外部端末からの内部機器へのアクセスをアクセス制御サーバが管理し、利用者に応じてアクセスできる内部機器を制限することが示されている。

【0004】

【発明が解決しようとする課題】一方、家庭内の各種機器をホームネットワークで接続し、コントロールするシステムが提案されており、これらについても適切なアクセス制御が必要であると考えられる。特に、家庭内の機器についてもインターネットを介する外部からのアクセスが可能となっており、これに対するアクセス制御も重要である。

【0005】ここで、家庭内の機器は、機器毎にその機能などが大きく異なっており、利用者毎にきめ細かなアクセス制御が重要と考えられる。

【0006】本発明は、上記課題に鑑みなされたものであり、きめこまかなアクセス制御を効果的に行えるアクセス制御システムを提供することを目的とする。

【0007】

【課題を解決するための手段】本発明は、内部ネットワークを介し接続された複数の機器と、前記複数の機器のそれぞれについて、制御内容のレベルに応じアクセスの可否を決定するアクセス管理情報を記憶し、前記複数の機器に対するアクセスを管理する管理サーバと、を含み、前記管理サーバは、外部通信ネットワークを介し行われる、外部からの前記複数の機器へのアクセスを制御することを特徴とする。

【0008】このように、制御内容のレベルに応じたアクセスを管理する管理サーバを設けることにより、きめこまかなアクセス管理を行うことができる。

【0009】また、本発明は、内部ネットワークを介し接続された複数の機器と、前記複数の機器についてのアクセス管理情報を記憶し、前記複数の機器に対するアクセスを管理する管理サーバと、を含み、前記管理サーバは、外部通信ネットワークを介し接続された機器の内の1つの機器による、あるいは、前記複数の機器の内の1つの機器による、他の機器が有するオブジェクトの使用を制御することを特徴とする。

【0010】このように、管理サーバが内部ネットワーク内の機器のオブジェクトの使用について管理することで、各機器のオブジェクトの適切な利用を図ることができる。

【0011】また、本発明は、内部ネットワークを介し接続された複数の機器と、前記複数の機器のそれぞれに

(3)

特開2003-69595

3

について、制御内容のレベルに応じアクセスの可否を決定するアクセス管理情報を記憶し、前記複数の機器に対するアクセスを管理する管理サーバと、を含み、前記管理サーバは、外部通信ネットワークを介し行われる、外部からの前記複数の機器へのアクセスを制御すると共に、外部通信ネットワークを介し接続された機器の内の1つの機器による、あるいは、前記複数の機器の内の1つの機器による、他の機器が有するオブジェクトの使用を制御することを特徴とする。

【0012】また、前記管理サーバは、利用者毎、または10 利用者のレベル毎にアクセスの可否またはオブジェクト使用の可否についてのデータを記憶していることが好適である。

【0013】

【発明の実施の形態】以下、本発明の実施形態について、図面に基いて説明する。

【0014】図1は、システムの全体構成を示す図である。自宅10には、例えば通信機能を有するコンピュータで構成される家庭内サーバ12が設置されている。また、この家庭内サーバ12には、ホームネットワーク14を介し、宅内機器16が接続されている。この宅内機器16は、エアコン、テレビ、ビデオ、オーディオ機器、パソコン、デジタルカメラなどの電子的制御可能な機器であり、複数接続することも可能である。家庭内サーバ12が、これらの宅内機器16へのアクセス権を制御する。なお、各宅内機器16は、基本的にそれぞれ個別にマニュアル操作が可能である。

【0015】自宅10の家庭内サーバ12には、外部ネットワーク30を介し、宅外機器20が接続されている。外部ネットワークは、例えばインターネットのような公衆回線を利用したネットワークである。また、宅外機器20は、ユーザが携帯する端末装置であり、携帯電話機や、PDA（パーソナル・デジタル・アシスタント）などが好適である。

【0016】このような構成により、ユーザが宅外機器20を携帯して、外出した場合、外出先から外部ネットワーク30を介し、自宅10の家庭内サーバ12に接続し、宅内機器の各種動作を制御することができる。

【0017】図2には、家庭内サーバ12の機能ブロックが示されている。アクセス制御テーブル作成部12aは、宅内機器16についてのアクセス権を管理するテーブルを生成する。作成されたテーブルは、アクセス制御テーブル12cとして記憶される。アクセス制御テーブル検査部12bは、必要に応じてアクセス制御テーブル12cの内容を検査する。

【0018】利用者テーブル作成部12dは、利用者毎のセキュリティレベルを規定するテーブルを生成する。作成されたテーブルは、利用者テーブル12hとして記憶される。利用者テーブル検査部12eは、必要に応じて利用者テーブル12hの内容を検査する。

4

【0019】機器テーブル作成部12fは、宅内機器16毎のセキュリティレベルを規定するテーブルを生成する。作成されたテーブルは、機器テーブル12iとして記憶される。機器テーブル検査部12gは、必要に応じて機器テーブル12iの内容を検査する。

【0020】また、利用者認証部12jは、外部ネットワーク30を介し、アクセスしてくる利用者について、登録された利用者かどうかを認証する。例えば、宅外機器20は、電子証明書を家庭内サーバ12に送付し、家庭内サーバ12はこの電子証明書により利用者を認証する。

【0021】図3には、宅外機器20の機能ブロックが示されている。利用者認証部20aは、宅外機器20を操作する利用者についての電子証明書を取得するとともに、これを家庭内サーバ12に供給する。アクセス可能オブジェクト選択部20bは、家庭内サーバ12から供給されるアクセス可能オブジェクトに応じ、利用者によって選択されたオブジェクトの情報を家庭内サーバ12に供給する。

【0022】図4には、宅内機器16の機能ブロックが示されている。機器テーブル登録データ転送部16aは、機器テーブル作成部12fに登録するためのデータを供給する。

【0023】図5には、機器テーブル12iの一例が示されている。この例では、宅内機器16として、デジタルカメラ（デジカメ）、ビデオレコーダ（ビデオ）、テレビ、サーバ（家庭内サーバ12）が挙げられている。家庭内サーバ12も、そのアクセス制御以外の機能は、宅内機器16としてのパソコンであり、機器テーブル12iに挙げられている。

【0024】そして、各宅内機器16について、セキュリティレベルが設定されるが、1つの機器について1つのセキュリティレベルではなく、その内容に応じて異なるセキュリティレベルが設定できるようになっている。すなわち、デジカメであれば、撮影、転送、コンテンツ1～3の5種類のオブジェクト別にセキュリティレベルが設定されている。ここで、撮影はデジカメのシャッター制御、転送はデジカメからの撮影データの転送、コンテンツ1～3は撮影コンテンツの閲覧を意味している。さらに、ビデオについては、再生、録画、テレビについては表示、サーバについては、保存、参照、コンテンツ4、5、6がオブジェクトとして挙げられている。このような各種のオブジェクトについて、個別にセキュリティレベルが設定される。ここで、オブジェクトセキュリティは、大中小の3段階となっている。

【0025】なお、API（アプリケーション・プログラム・インタフェース）は、各種動作を行うプログラムで、外部からの指令でAPIの関数を呼び出して所定の処理を実行させる。すなわち、外部からの指令でAPIを指定することで、対応する動作が実行される。

(4)

特開2003-69595

5

【0026】図6には、利用者テーブル12hの一例が示されている。このように、各利用者A、B、C、Dに対し、セキュリティの大中小が割り当てられている。

【0027】図7には、アクセス制御テーブル12cの一例が示されている。このアクセス制御テーブル12cでは、オブジェクトセキュリティの大中小と利用者セキュリティの大中小によって、アクセスを許可するかどうかを示している。図中○が許可、×が不許可である。この例ではオブジェクトセキュリティが利用者セキュリティ以下の場合にアクセスを許可するようになって

【0028】図8は、宅外機器20の認証のフローチャートを示しており、宅外機器20からのアクセスがあった場合には、まず宅外機器からの利用者を認証する（S101）。次に、利用者テーブル12hを検索し、認証された利用者のセキュリティを決定する（S102）。

【0029】図9には、宅外機器からのアクセスの時のフローチャートを示しており、まず宅外機器20から宅内機器16へのアクセス要求を受け付ける（S201）。次に、アクセス制御テーブル12cを検索し、利用者が利用可能なオブジェクトセキュリティを取得する（S202）。取得したオブジェクトセキュリティを持ち、かつ要求された機器のオブジェクトを取得する（S203）。取得した複数のオブジェクトを宅外機器20に提示する（S204）。そして、宅外機器20が、提示されたオブジェクトの中から希望のものを選択して実行する（S205）。すなわち、機器テーブル12iの中で宅外機器20で選択されたものが実行される。なお、選択されたものが処理動作の場合、APIが指定され、その動作が宅内機器16において実行される。

【0030】図10には、予め利用者の利用できるオブジェクトについての情報を提示する場合のフローチャートを示す。このフローチャートによれば、まず宅外機器からの利用者を認証する（S301）。次に、利用者テーブル12hを検索し、利用者セキュリティを決定する（S302）。そして、利用者セキュリティを満足するオブジェクトを利用者へ返送する（S303）。このようにして、宅外機器20において、利用者認証終了後に、その利用者について利用可能なオブジェクトの情報が得られる。従って、利用者は提供された情報から、どの処理を行うかを決定することができる。

【0031】このように、本実施形態によれば、(1)宅外機器からAPIを指定することで、宅内機器を直接制御することができるため、特別の内部機器操作手段を持つ必要がない、(11)操作のみでなくコンテンツについてもそのアクセス権を管理することができる、(111)アクセス権そのものにレベルを持たせているため、きめ細かな制御が行える、という特徴が得られる。

6

【0032】次に、他の実施形態について説明する。図11には、システムの全体構成を示してある。自宅110、ホームネットワーク114、宅外機器120、外部ネットワーク130は、基本的に上述の実施形態と同一である。そして、自宅110内の外部ネットワーク130とホームネットワーク114の間には、アクセス管理サーバ112が配置されている。また、宅内機器として、オブジェクトクライアントとして機能する宅内機器116と、オブジェクトサーバとして機能する宅内機器118が設けられている。なお、すべての宅内機器は、宅内機器116または宅内機器118のいずれになることもできる。

【0033】図12には、アクセス管理サーバ112の機能が示されている。アクセス管理テーブル作成部112aは、宅内機器116についてのアクセス権を管理するテーブルを生成する。作成されたテーブルは、アクセス管理テーブル112dとして記憶される。アクセス管理テーブル検査部112bは、必要に応じてアクセス管理テーブル12cの内容を検査する。また、利用者認証部112cは、宅内機器116、118をアクセスする利用者について、認証する。

【0034】図13には、宅内機器118の機能ブロックが示されており、利用者認証部118aは、その宅内機器118の利用者を認証する。また、オブジェクトクライアント118bは、利用者の指示に基づいて、宅内機器116のオブジェクトに対しオブジェクトのメソッドを呼び出す。

【0035】図14には、宅内機器116の機能ブロックが示されており、メソッド情報転送部116aはアクセス管理テーブル112dに必要な情報をアクセス管理サーバ112に転送する。オブジェクトサーバ116bは、メソッド要求を受けたらアクセス管理サーバへ利用者のアクセス権があるかを問い合わせ、問い合わせ結果において、権利がある場合に要求に応え、要求されたオブジェクトについてアクセスを許可する。

【0036】図15には、オブジェクトアクセス管理テーブル112dの構成が示されている。このように、オブジェクトの種類(a、b、c)毎に、利用者別にアクセスを許可するかどうかのデータが記憶されている。

【0037】次に、このようなシステムの動作について、説明する。図16に示すように、宅内機器116のオブジェクトサーバ116bは、提供可能なメソッドをアクセス管理サーバ112に登録する（S401）。これによって、図15に示すような管理テーブル112dが作成される。

【0038】次に、図17にオブジェクトの利用の動作について示す。まず、宅内機器118のオブジェクトクライアント118bが宅内機器116のオブジェクトサーバ116bへメソッドの要求メッセージを送付する（S501）。オブジェクトサーバ116bがアクセス

(5)

特開2003-69595

7

管理サーバ112へメソッド要求利用者のアクセス権を問い合わせる(S502)。次に、アクセス管理サーバ112がアクセス権を検査してアクセスの可否を応答する(S503)。そして、オブジェクトサーバ116bがアクセスの可否を受け取り、メソッド要求を認めるか否かを決定する(S504)。

【0039】このようにして、オブジェクトクライアント118bの要求に応じて、オブジェクトサーバ116bがアクセス管理サーバ112に、その可否を問い合わせ決定する。

【0040】この例では、宅内機器118にオブジェクトクライアント118bがあり、ホームネットワーク114に接続されている場合を説明したが、これを外部ネットワーク130を介して接続してもよい。

【0041】従って、オブジェクト毎にアクセス制御が可能になる。つまり、ビデオの再生や録画などの機器操作毎にセキュリティを設定することができる。さらに、それらの操作の組合せに対してセキュリティを設定することが可能になる。

【0042】

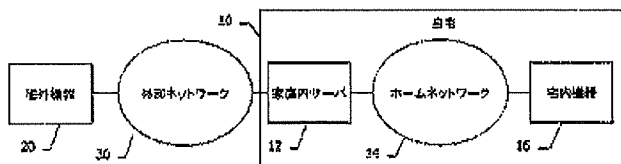
【発明の効果】以上説明したように、制御内容のレベルに応じたアクセスを管理する管理サーバを設けたことにより、きめこまかなアクセス管理を行うことができる。

【0043】また、管理サーバが1つの機器による内部ネットワーク内の他の機器のオブジェクトの使用について管理することで、各機器のオブジェクトの適切な利用を図ることができる。

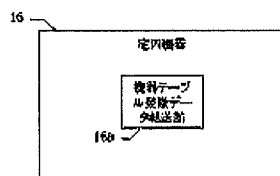
【図面の簡単な説明】

【図1】 実施形態の全体構成を示すブロック図である。

【図1】



【図4】



【図6】

| 制御テーブル 利用権/セキュリティ | |
|----------------------|---|
| A | 大 |
| B | 中 |
| C | 小 |
| D | 小 |

【図7】

| アクセス制御 テーブル | 利用権 セキュリティ |
|----------------|---------------|
| 大 | 大 |
| 中 | 中 |
| 小 | 小 |

8

*【図2】 家庭内サーバの機能を示す図である。

【図3】 宅外機器の機能を示す図である。

【図4】 宅内機器の機能を示す図である。

【図5】 機器テーブルの構成を示す図である。

【図6】 利用者テーブルの構成を示す図である。

【図7】 アクセス制御テーブルの構成を示す図である。

る。

【図8】 利用者認証の処理を説明するフローチャートである。

10 【図9】 オブジェクト利用可否を決定する処理を説明するフローチャートである。

【図10】 セキュリティレベルを提示する処理を説明するフローチャートである。

【図11】 他の実施形態の構成を示すブロック図である。

【図12】 アクセス管理サーバの構成を示す図である。

【図13】 宅内機器118の構成を示す図である。

【図14】 宅内機器116の構成を示す図である。

20 【図15】 オブジェクトについてのアクセス管理テーブルを示す図である。

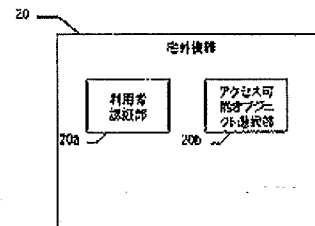
【図16】 オブジェクトのメソッド登録に関するフローチャートである。

【図17】 アクセル可否についてのフローチャートである。

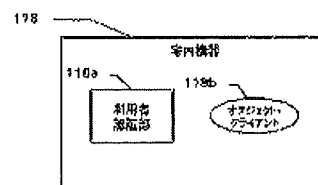
【符号の説明】

10、110 自宅、12 家庭内サーバ、14、114 ホームネットワーク、16、116、118 宅内機器、20、120 宅外機器、30、130 外部ネットワーク、112 アクセス管理サーバ。

【図3】

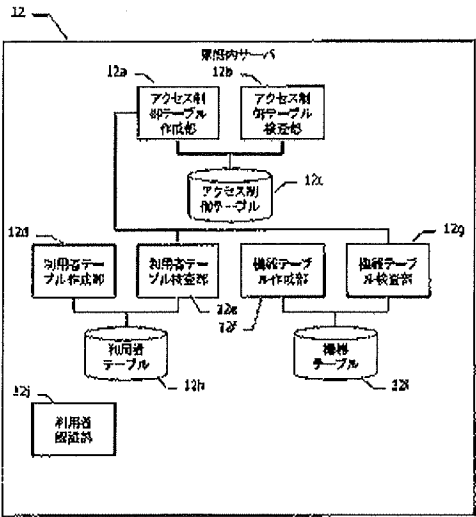


【図13】



(6) 特開2003-69695

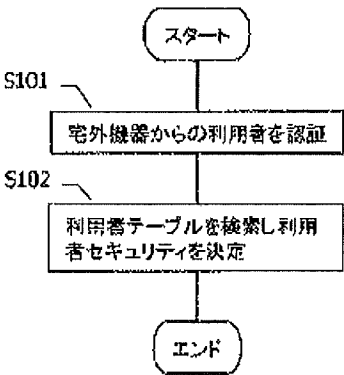
【図2】



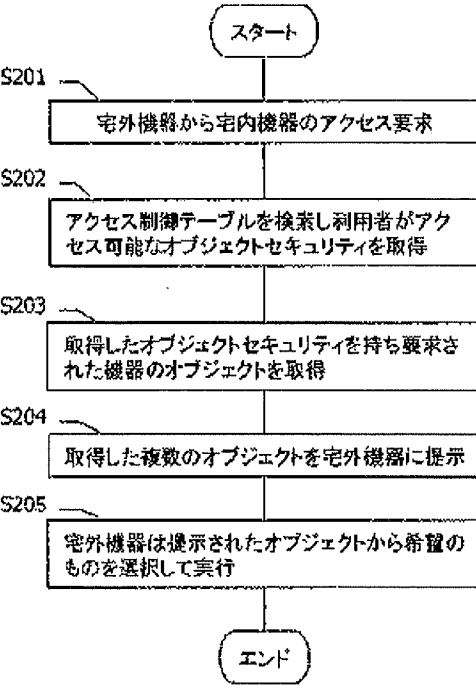
【図5】

| 権限テーブル | | | |
|--------|---------|--------------|------|
| 機器 | 権限/コンテナ | オブジェクトセキュリティ | API |
| カメラ | 撮影 | 大 | API1 |
| | 送信 | 大 | API2 |
| | コンテナ | 小 | - |
| ビデオ | 再生 | 中 | - |
| | 録画 | 中 | - |
| | 削除 | 中 | API3 |
| サーバ | 表示 | 小 | API4 |
| | 実行 | 大 | API5 |
| | 削除 | 小 | API2 |
| サーバ | コンテナ | 小 | - |
| | コンテナ | 中 | - |
| | コンテナ | 大 | - |

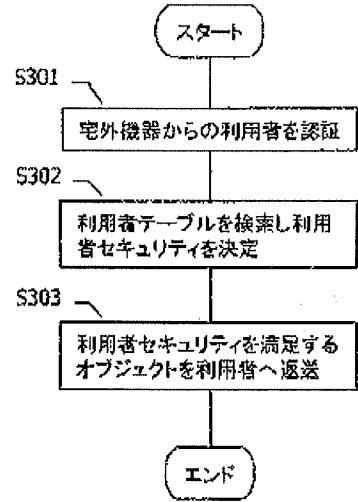
【図8】



【図9】



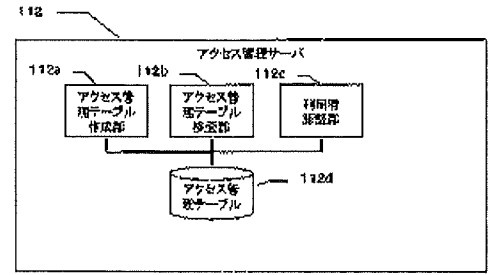
【図10】



【図15】

| オブジェクトアクセス管理テーブル | | | |
|------------------|---|---|---|
| オブジェクト | a | b | c |
| 利用者A | ○ | × | ○ |
| 利用者B | ○ | ○ | ○ |
| 利用者C | × | ○ | × |

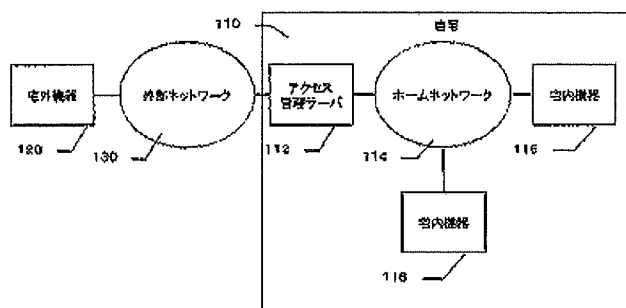
【図12】



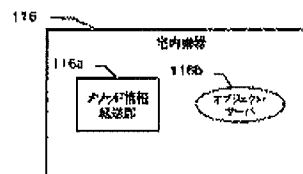
(7)

特開2003-69695

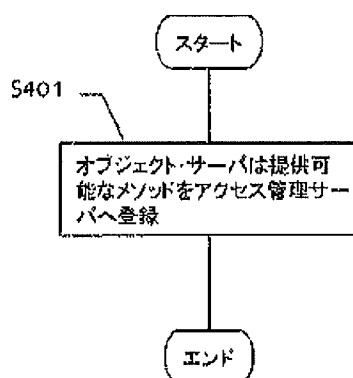
【図11】



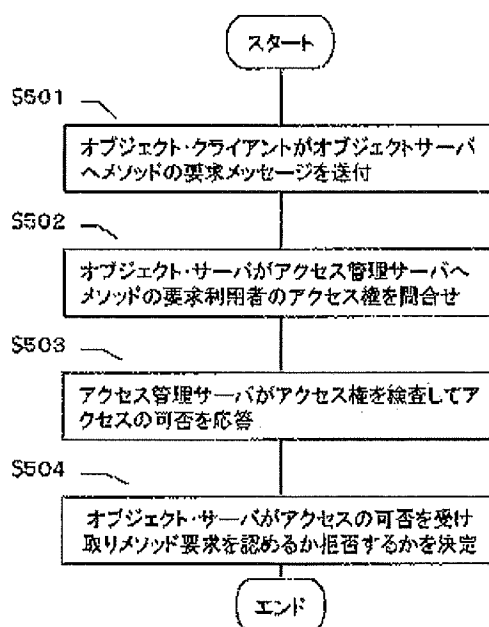
【図14】



【図16】



【図17】



フロントページの続き

Fターム(参考) 5B017 AA07 BA06 CA16
 5B085 AE06 BG07
 5K030 GA15 HA08 HD03 HD06 KA04
 LD29
 5K033 AA08 BA01 CB08 DA06 DB12
 DB14 DB16 DB18
 5K048 AA15 BA01 BA13 DA05